

**AFFIDAVIT OF FBI SPECIAL AGENT ADAM STRODE**

I, Adam Strode, having been duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent (“SA”) of the Federal Bureau of Investigation (“FBI”). I have been so employed since 2015. I am currently assigned to the Boston Division, Worcester Resident Agency. My duties include the investigation of violations of the United States Code. Pursuant to my employment with the FBI, I have participated in various criminal investigations, and have been the affiant on federal search warrants and court orders. I have directly participated in numerous criminal investigations for violations of federal law to include bank fraud, identity theft, child exploitation, and healthcare fraud. I have received on-the-job training and have attended FBI-sponsored training courses on the investigation of criminal violations. I have conducted and participated in the execution of search and arrest warrants, physical surveillance, interviews of cooperating witnesses, and reviews of documents and evidence.
2. I submit this affidavit in support of an application for a warrant pursuant to Federal Rule of Criminal Procedure 41 authorizing the search of premises located at 919 Pleasant Street, Worcester, Massachusetts 01602 (the “SUBJECT PROPERTY”), as more fully described in Attachment A.
3. Based on the facts presented in this affidavit, there is probable cause to believe that Gregory LISBY has committed violations of Title 18, United States Code, Section 2252A(a)(2)(A), the receipt of child pornography, and Title 18, United States Code, Section 2252A(a)(5)(B), the possession of child pornography, collectively, the “SUBJECT OFFENSES.”

4. As described below, there is also probable cause to believe that the SUBJECT PROPERTY contains evidence, instrumentalities, fruits of crime and contraband as more fully described in Attachment B. The evidence described in Attachment B includes evidence maintained in electronic format on any computer (or other device capable of storing data) within the SUBJECT PROPERTY. The methods by which the electronic information will be searched are more fully set forth in the “Searching and Seizing Computer Evidence” section of this Affidavit.
5. The information contained in this affidavit is based in part on my personal involvement and knowledge of this investigation, information obtained by other agents and investigators involved in this matter, information provided by Microsoft Corporation, and other information gathered during the course of the investigation. This affidavit does not contain every fact known to me with respect to this investigation. Rather, it contains those facts that I believe necessary to establish probable cause for the issuance of the requested search warrant.

#### **RELEVANT STATUTES**

6. Title 18, United States Code, Sections § 2252A(a)(2)(A) and (b)(1) prohibits a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
7. Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting or

conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

8. “Child pornography” is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.
9. The term “minor” is defined in 18 U.S.C. § 2256(1) as any person under the age of eighteen years.

#### **THE NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN**

10. The National Center for Missing and Exploited Children (“NCMEC”) was established in 1984 as a private, nonprofit 501(c)(3) organization to provide services nationwide for families and professionals in the prevention of abducted, endangered, and sexually exploited children. NCMEC’s mission is to help prevent child abduction and sexual exploitation, help find missing children, and assist victims of child abduction and sexual exploitation, their families, and the professionals who serve them. Pursuant to its mission and its congressional mandates (see 42 U.S.C. § 5771 et seq.; 42 U.S.C. § 11606; 22 C.F.R. § 94.6), NCMEC serves as a clearinghouse of information about missing and exploited children and operates a

“CyberTipline” (aka “Cybertip”) that the public may use to report Internet-related child sexual exploitation.

11. The Congressionally-mandated CyberTipline is a reporting mechanism for incidents of child sexual exploitation, including child pornography, online enticement of children for sex acts, molestation of children outside the family, sex tourism of children, child victims of prostitution, and unsolicited obscene material sent to a child. Reports may be made 24-hours a day, 7 days a week either online or by calling a toll free number.

12. In 1996, the U.S. Congress established the Exploited Child Unit (“ECU”) within NCMEC.

In addition to handling reports received via the CyberTipline, the ECU serves as a technical and informational resource for law enforcement. As such, the ECU is highly experienced in identifying child pornography.

13. The ECU maintains a database of images and their hash values that depict identified victims of child pornography.<sup>1</sup> In response to a law enforcement submission of an “Initial Hash Value Comparison Report,” NCMEC reports whether the images contain an “Identified Child” or “Unrecognized Hash Value.” According to NCMEC, an “Identified Child” signifies that “[t]hese exact hash values are associated with an image/video which appears to depict at least one (1) child previously identified by law enforcement. Please be advised that these hash values may be associated with apparent child pornography images/videos as well as files that do not contain apparent child pornography.” An “Unrecognized Hash Value”

---

<sup>1</sup> A “hash algorithm” is used to calculate the hash value of a file. For all practical purposes, the output of this hash algorithm uniquely identifies the input. In this case, the output (referred to as a hash value) uniquely identifies a photograph or video. So, if two photographs have the same hash value, the two photographs are identical. The possibility of a hash algorithm calculating identical values for non-identical files, known as a collision, is minute; for example, the probability of this occurring with the SHA1 algorithm is  $2^{80}$  operations to produce a 50% probability of finding a collision.

signifies that “[t]hese exact hash values are associated with images/videos that have not yet been submitted to NCMEC’s Child Recognition and Identification System.”

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO CONSUME CHILD PORNOGRAPHY**

14. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who utilize web-based services to access with intent to view and possess, collect, receive, or distribute images of child pornography (*i.e.*, consumers of child pornography), as follows:

- a. Consumers of child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media.
- b. Consumers of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, videos, books, drawings, other visual media, and, increasingly, digital format. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Consumers of child pornography almost always possess and maintain their child pornographic material (whether stored in hard copy or digitally) in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children often retain pictures, videos, digital media,

and other documentation of child pornography and child erotica for many years.<sup>2</sup>

Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

- d. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and other digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.<sup>3</sup>
- e. Consumers of child pornography also may correspond with and/or meet others to share information and materials; often maintain correspondence from other child pornography consumers; conceal such correspondence as they do their sexually explicit material; and often maintain the contact information of individuals with whom they have been in contact and who share the same interests in child pornography.
- f. Consumers of child pornography prefer not to be without access to child pornography for any prolonged time period. This behavior has been documented

---

<sup>2</sup> See *United States v. Morales-Aldahondo*, 524 F.3d 115, 117-19 (1st Cir. 2008) (3-year delay between last download and warrant application not too long, given affiant testimony that consumers of child pornography value collections and thus often retain them for a period of time, and consumers who use computers to access child pornography are likely to use computers to store their collections).

<sup>3</sup> See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

by law enforcement officers involved in the investigation of child pornography throughout the world.

15. These offenders obtain and/or traffic in materials depicting children engaged in sexually explicit conduct through many sources and by several methods and means. These sources, methods and means include, but are not limited to, the following:

- a. Downloading via the Internet and other computer networks. (Web sites, peer-to-peer file sharing networks, newsgroups, electronic bulletin boards, chat rooms, instant message conversations, e-mail, etc.) via several devices to include but not limited to: documents (written or digital), computers, tablets, smartphones, and gaming systems;
- b. The use of anonymizing services such as TOR, makes it more difficult for the user's Internet activity to be traced.
- c. Receipt from commercial sources within and outside of the United States through shipments, deliveries and electronic transfer; trading with other persons with similar interests through shipments, deliveries and electronic transfer, including but not limited to email exchanges; and
- d. Producing and manufacturing these materials during actual contact with children or manipulating children into creating such materials and providing them to the perpetrator.

## **FACTS ESTABLISHING PROBABLE CAUSE**

### **A. Identification of Child Pornography within the TARGET ACCOUNT**

16. On December 17, 2018 at 17:05:15 UTC, NCMEC received CyberTip Report #44377012 from Microsoft Corporation (“Microsoft”), a registered Electronic Service Provider.<sup>4</sup>
17. According to Cybertip Report #44377012, on December 17, 2018 at 14:58:46 UTC, a digital file with the file name “6aae7237-fb28-40a3-85d6-52cee6b43516.jpg” (hereinafter the “SUBJECT FILE”) was uploaded to servers owned by Microsoft Corporation, specifically the OneDrive service, by an individual using the screen/user name “844427362124387,” i.e. the TARGET ACCOUNT. The user of the TARGET ACCOUNT utilized IP address 71.87.214.73 to upload the SUBJECT FILE. According to CyberTip Report #44377012, a Microsoft employee viewed the contents of the SUBJECT FILE and determined that it contained child pornography, then reported the upload to NCMEC.
18. NCMEC transmitted the SUBJECT FILE, along with CyberTip Report #44377012, to Massachusetts State Police on January 4, 2019 at 18:34:06 UTC.
19. I reviewed the SUBJECT FILE identified by Microsoft. The SUBJECT FILE depicts two males engaged in anal sex. Male1 appears to be kneeling on the ground facing a bed, resting his torso on the mattress. Male2 is kneeling behind Male1 and appears to be penetrating Male1’s anus with his penis. The penis of Male2 is partially visible. The faces of Male1 and Male2 are both partially visible. Neither boy has visible facial hair or body hair. Based upon their size and the lack of facial and body hair, I estimate that both boys are between 11 and 14 years old.

---

<sup>4</sup> An “Electronic Communication Service Provider” (“ESP”) is defined in 18 U.S.C. § 2510(15) as any service which provides to users thereof the ability to send or receive wire or electronic communications.



20. On August 27, 2019, Microsoft Corporation provided the contents of the TARGET ACCOUNT in response to federal search warrant 19-mj-4468-DHH, issued on August 8, 2019.
21. Investigators reviewed the data provided by Microsoft for the TARGET ACCOUNT and identified approximately 180 images that appear to depict child pornography. Investigators also found approximately 15 videos that appear to depict child pornography.
22. Data from Microsoft was categorized as “preserved” and “current.” Within both directories, I located two folders named “Inside” and “CADE” that contained images. Based upon my training and experience, I believe that the designation “current” indicates that the file was active in the account as of the date Microsoft prepared the data, on approximately August 15, 2019. The data was produced to the FBI on August 27, 2019.
23. Specifically, within the “Inside” folder, which appears to have been added to the OneDrive account on December 17, 2018, there were approximately 140 images that, based upon my review, appear to depict child pornography. The “upload IP” address for all of the images contained within the “Inside” folder was 71.87.214.73, which is the same IP address used to upload the SUBJECT FILE.
24. Amongst the files saved within the “Inside” folder was a file named “twlba5j7o5gj5.onion.jpg” This file appears to me to contain the same image as the SUBJECT FILE from Microsoft’s initial Cybertip, more particularly described in paragraph 17, though it has a different filename. A comparison of the hash values of those two files confirmed that they are identical.
25. On September 4, 2019, the FBI computed the hash value of 146 files from the “Inside” folder. Those hash values were submitted to NCMEC.

26. On September 4, 2019, NCMEC sent a response to the FBI via an “Initial Hash Value Comparison Report”, which identified 33 of those submitted hash values as containing an “Identified Child.” Specifically, the file named “twlba57oo5g4kj5.onion.jpg” depicts two males engaged in anal sex. Male1 is naked and his face is visible. Male1’s anus is being penetrated by Male2’s penis. Male2’s face is not visible. Male1 has a small build and no facial or body hair. I estimate Male1’s age to be between 8 years old and 12 years old. Only a portion of Male2’s stomach, leg, hand, and penis are visible. Based on Male2’s size and visible body hair, I estimate that Male2 is an adult over the age of 18.
27. The contents of the TARGET ACCOUNT also contained a folder entitled “CADE,” which appears to have been added to the TARGET ACCOUNT on December 13, 2018. The “upload IP” address for all of the files in the “CADE” folder was 71.87.214.73, which is the same IP address used to upload the SUBJECT FILE.
28. I reviewed the contents of the CADE file and observed approximately 50 images that appear to be of one unidentified minor male. The majority of these images contain apparent child pornography. For example, a file named “467575ce-efbf-41dc-aa7c-1ea47c4882ca” depicts a naked male standing with his hands behind his head and his genitals fully visible. Based upon his slight frame, he appears to be approximately 12-15 years old. The image appears to be a picture taken by the boy of his own reflection in the mirror. His face is fully visible.<sup>5</sup>
29. The CADE file also included several videos. The video file named “766e2b2c-5bac-4285-9cf6-9c44ef9b4310” appears to depict the same male as seen in the still images. In the video, the boy is naked and masturbating on a bed. The boy’s face and penis can be seen.

---

<sup>5</sup> This image has been provided to the Court for review. It will be preserved by the U.S. Attorney’s Office for the duration of the pendency of this matter, including any relevant appeal process.

30. On September 4, 2019, a NCMEC Initial Hash Value Comparison Report was generated containing the hash values from 54 files from the “CADE” folder. NCMEC responded that all of the hash values were unrecognized.
31. The records provided by Microsoft Corporation for the TARGET ACCOUNT included evidence of the download and use of a TOR Browser.<sup>6</sup> In addition, a number of the files containing apparent child pornography within the folder entitled “Inside” have file names that include “.onion.jpg.” “.onion”, is a domain suffix designating an anonymous onion service (also known as a “hidden service”) that can be reached via the TOR network. Based on my training and experience, I know that individuals will use TOR to share files containing child pornography in order to minimize detection of their online activity.

B. Use and control of the TARGET ACCOUNT

32. Account subscriber data provided by Microsoft for the TARGET ACCOUNT listed the name as “Greg Lisby,” with a sign-in name of “glisby@gmail.com” and an account creation date of May 19, 2009.
33. Further review of the data provided by Microsoft identified several word documents that appear to belong to Greg LISBY. Word document “2018-Greg Lisby-School 3” appears to be LISBY’s resume. The document appears to have been added to the TARGET ACCOUNT August 13, 2018. The top of the document states, “Gregory C. Lisby, 919 Pleasant St. Worcester, MA 01602, (401) 965-1413, [glisby@gmail.com](mailto:glisby@gmail.com).” A separate Word document entitled “Document 1” appears to be an introduction letter written by LISBY for an online

---

<sup>6</sup> TOR (The Onion Router) is free and open-source software for enabling anonymous communications. TOR directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays to help conceal a user’s location and usage from anyone conducting network surveillance or traffic analysis. In order to access TOR specific websites a user needs to use a TOR browser or a proxy gateway.

course. The document states “...My name is Greg Lisby, and I recently applied to the PBTLE in Early Childhood Education.” The letter then further states, “...If I could teach any grade, I would love to be a kindergarten teacher. The joy, spontaneity, and openness to learning of younger children is what attracts me to early childhood education. Plus, the energy of the kids, and the energy required of the teacher is exhilarating and tiring.” That file appears to have been added to the TARGET ACCOUNT on September 3, 2018 and modified on September 28, 2018. A file entitled “Charge Letter 2 – 1-21-18” is a Word document which appears to have been added to the TARGET ACCOUNT on approximately January 23, 2018. It appears to be a letter from the Intake Coordinator for the diocese and is addressed to “The Rev. Gregory C. Lisby, 14 Whitman Rd, Worcester, MA 01609-1728.”

C. Identification of the SUBJECT PROPERTY

34. On or about January 22, 2019, Charter Communications provided the following records in response to a subpoena requested by Massachusetts State Police for customer records related to the assignment of IP address 71.87.214.73 on December 17, 2018 at 14:58:46 UTC:

Service Address: 919 Pleasant Street Worcester, MA

Lease record: November 4, 2018 through January 20, 2019

Name: Timothy Burger

Billing address: 919 Pleasant Street Worcester, MA 01602

Contact Email: [REDACTED]

Active Charter Identities: [REDACTED]@charter.net; [REDACTED]@charter.net.

Primary Phone Number: 401-[REDACTED]

35. On May 23, 2019, investigators conducted a public records database search for 919 Pleasant Street, Worcester, Massachusetts. That query identified Timothy Burger, born 1978, as

living at this address from August 2015 to April 2019. That same query also identified LISBY as living at 919 Pleasant Street from August 2015 to May 2019.<sup>7</sup>

36. An internet search of publicly available databases indicates that Timothy Burger and LISBY are married.
37. Queries of the Criminal Justice Information System (“CJIS”) yielded negative results for both Burger and LISBY.
38. On May 23, 2019, a query of the Massachusetts Registry of Motor Vehicles (“RMV”) database identified an active Massachusetts license issued to Timothy H. Burger with an address of 919 Pleasant Street, Worcester. The query of the RMV database also identified an active Massachusetts license issued to LISBY with an address of 919 Pleasant Street, Worcester.
39. According to the RMV, a 2017 red Toyota Prius sedan, MA Reg: 5XX463 (the “Prius”) is registered to LISBY. Investigators observed the Prius parked in the driveway at 919 Pleasant Street, Worcester on September 8, 2019, and September 10, 2019. The Prius, an electric hybrid vehicle, appeared to be plugged into an outlet at the home.
40. Publicly available information online indicates that LISBY works as a kindergarten teacher for the Holyoke Public Schools.

#### **MICROSOFT ONEDRIVE**

41. Microsoft OneDrive provides remote, “cloud,” or web based, storage of electronic files.

Microsoft advertises on its website that “OneDrive is cloud storage that you can get to from

---

<sup>7</sup> An Episcopal church is located at 921 Pleasant Street in Worcester, immediately adjacent to 919 Pleasant Street. The website for that church indicates that Reverend Timothy Burger is the rector of the church. Upon information and belief, Gregory Lisby is also an ordained minister and served as the rector of a different Episcopal church in Worcester from 2015-2018, although it does not appear that he is formally serving in that capacity presently. Investigators will make every effort to avoid and/or minimize the disclosure of any privileged communications that may be encountered during the search.

anywhere. It helps you stay organized, access your important documents, photos, and other files from any device, and share those files with friends, family, or coworkers. The OneDrive folder on your computer always keeps your files up-to-date. Anything you add or edit in there gets synced via the cloud to your other devices or people you've shared with.” “Access your files anywhere you have internet access. Log in at OneDrive.com to view and share any file or create Office documents right from your browser.” “On your phone or tablet,” “No matter where you are, your files are always within reach with the OneDrive mobile apps for Android, iOS, and Windows Phone.”

<https://download.microsoft.com/download/C/1/3/C13BEF63-BE65-415B-97D0-2C7506AE475E/Getting%20started%20with%20OneDrive.pdf/> (last visited August 5, 2019). Because the files are remotely stored, they are accessible even if the user loses the device on which they were originally stored.

### **SEARCHING AND SEIZING COMPUTER EVIDENCE**

42. Computer hardware, other digital devices, software, and electronic files may be important to a criminal investigation in two distinct ways: (1) the objects themselves may be contraband, evidence, instrumentalities, or fruits of a crime; and / or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data.
43. I know from training and experience that computers and magnetic and optical media are used to store information. In addition to the above mentioned image files, that information often includes data files of other persons engaged in similar activities with minors, and lists of other exploited juveniles, as well as records of correspondence and conversations (printed or electronic) with such persons.

44. In this case, the search warrant application requests permission to search and seize digital media files of child pornography and child erotica, as further described in Attachment B, including those items that may be stored on a computer, digital device or on electronic media. The images involving sexual conduct of minors constitute both evidence of crime and contraband.

45. I know from training and experience that computer systems commonly consist of computer processing units (“CPUs”), hard disks, hard disk drives, display screens, keyboards, printers, modems (used to communicate with other computers), electronic cables, and other forms of magnetic and optical media contain computer information. In addition, the specific transmission of computerized imagery indicates the possible use of portable hard drives, USB storage drives, CD-ROM / DVD drives, compact laser disks, image scanning devices, still cameras, lighting equipment, video cameras or camcorders, VCRs, digital-analogue translation devices, and the software (computer programming) necessary to operate them.

46. Based on my training, experience, and information provided by other law enforcement officers, I know that many smartphones (which are included in Attachment B’s definition of “computer hardware”) can now function essentially as small computers. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a vast range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

47. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or years

after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

- a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.
- b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

48. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as



they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

**NEED FOR COMPUTER EQUIPMENT TO BE SEIZED  
AND SEARCHED OFF-SITE**

49. This affidavit also requests permission to seize the computer hardware and storage media that may contain the digital media files of child pornography if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site. I believe that, in this case, the computer and digital hardware is a container for evidence, a container for contraband and also itself an instrumentality of the crime under investigation.

50. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media (“computer equipment”) be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

a. The volume of evidence — storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months,

depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. Technical requirements — analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even “hidden,” deleted, compressed, or encrypted files.

Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a “booby trap.” Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

51. The premises may contain computer equipment whose use in the crime(s) or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner’s knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine

their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

52. Based on my training and experience, and discussions with members of the FBI CART, members of the FBI Boston Division's cyber squad, members of the Homeland Security Investigations' ("HSI") Cyber Crimes Unit, and the Massachusetts State Police Computer Crimes Unit, I know that a qualified computer specialist is required to properly retrieve, analyze, document and authenticate electronically stored data, and to prevent the loss of data either from accidental or deliberate programmed destruction. To do this work accurately and completely requires the seizure of (1) all computer equipment and peripherals, which may be interdependent; (2) the software to operate the computer system(s); (3) the instruction manuals, which contain directions concerning the operation of the computer system(s) and software programs; and, (4) all internal and external data storage devices. Each of the seized items should be searched in a laboratory or controlled environment.
53. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a significant amount of time. Indeed, computer specialists, using exacting data search protocols, must often recover hidden, erased, compressed, password-protected, or encrypted files in order to find evidence of criminal activity. Moreover, many commercial computer software programs save data in unique formats that are not conducive to standard data searches. This requires additional effort by specialists to review such data for evidence of a crime. Finally, many users try to conceal criminal evidence by storing files in random order with deceptive file names. This requires specialists to examine all of a user's stored data to determine which particular files are relevant and within the scope of the search

warrant. This process can take a substantial amount of time depending on the volume of data stored.

54. Because computer evidence is extremely vulnerable to tampering or destruction, both from external sources or from destructive codes imbedded in the system as “booby traps,” a controlled environment is essential to a complete and accurate analysis.
55. For the reasons described in the Computer Evidence section of this affidavit, it is necessary to seize all computers, data storage devices and related equipment, as described in Attachment B. It is further necessary to search such equipment in a controlled environment, off-site. Given the potential for large quantities of data, a complete forensic examination of the seized items will take longer than fourteen days.

#### **RETURN OF SEIZED COMPUTER EQUIPMENT**

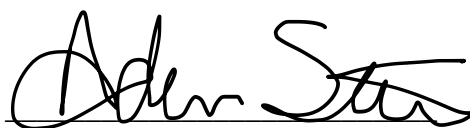
56. To the extent practical, if persons claiming an interest in the seized computers so request, I will make available to those individuals copies of requested files (so long as those files are not considered contraband) within a reasonable time after the execution of the search warrant. In addition, as soon as practical, those items of hardware and software no longer required for the purpose of analysis or copying of items authorized to be seized, or for the preservation of the data and/or magnetic evidence, will be returned to the party from which they were seized, so long as such items do not constitute contraband.

#### **CONCLUSION**

57. Based on the foregoing, I submit that there is probable cause to believe that LISBY has committed violations of Title 18, United States Code § 2252A(a)(2)(A) and (a)(5)(B), namely the receipt and possession of child pornography.

58. Further, there is probable cause to believe that the SUBJECT PROPERTY, as described more fully in Attachment A, contains evidence of crimes; contraband, fruits of crime, or other items illegally possessed; and constitutes property designed for use, intended for use, or used in committing the SUBJECT OFFENSES, as specifically detailed in Attachment B, hereto.

Sworn to under the pains and penalties of perjury,



Special Agent Adam Strode  
Federal Bureau of Investigations

Subscribed and sworn to before me this 11th day of September, 2019.



Hon. David H. Hennessy  
United States Chief Magistrate Judge



I have reviewed images described above in Paragraphs 19,24,28, and 29 above, and a still shot image from the video described in Paragraph 29, and I find probable cause to believe that those images depict minors engaged in sexually explicit conduct. The U.S. Attorney's Office shall preserve the images provided to the Court for the duration of the pendency of this matter, including any relevant appeal process.



Hon. David. H. Hennessy  
Chief United States Magistrate Judge

